GDPR SUBJECT ACCESS REQUEST TO MEDICAL RECORDS

Document Control

A. Confidentiality Notice

This document and the information contained therein is the property of Aspiro Healthcare.

This document contains information that is privileged, confidential or otherwise protected from disclosure. It must not be used by, or its contents reproduced or otherwise copied or disclosed without the prior consent in writing from our organisation

B. Document Details

Author and Role:	Paul Couldrey, Data Protection Officer
Current Version Number:	V1
Current Document Approved By:	Partnership Board
Date Approved:	13.06.2019

C. Document Revision and Approval History

Version	Date	Version Created By:	Version Approved By:	Comments
V1	01.10.18	Paul Couldrey	Partnership Board	

On behalf of Aspiro Healthcare, PCIG Consulting Limited has developed and written this guidance with the assistance of many member practices/LMCs and online resources, including: -

Winterton Medical Practice, The Ridgeway Surgery, Nidderdale Group Practice, Loomer Medical Group, Trent Vale Medical Practice, Oakenhall Medical Practice, St Pauls Surgery/Causeway Green Surgery, Westcount Medical Centre, Walsall LMC Members, Sandwell LMC Members, Dudley LMC Members, The BMA online resources and Dr Paul Cundy (GPC GDPR lead).

Contents

Flow Chart – Access to Medical Records Request

1. Receive request for access to Medical Records
2. SARs can be made electronically, in writing or verbally.
3. Complete Access to Medical Record Request form.

1. Does request provide a clear purpose? Is it from an Insurer?
2. Is the request under GDPR or AMRA
3. Is the requestor asking for copies of entire records or for specific dates
4. Is consent included – if patient does not have capacity – has evidence of Enduring Power of Attorney, Lasting Power of Attorney or a Court Appointed Deputy been included, have you checked the ID of the requestor?

Yes

No

1. Under GDPR – no Fee unless excessive or repeat request when a charge would be applicable
2. Under AMRA – Fee applies

Clarified

Contact Requestor to clarify – negotiate request if possible to date range rather than entire record

Use letter template

No

If still unable to clarify any/all:

1. Clear purpose
2. GDPR or AMRA
3. Evidence of consent

= Contact DPO to discuss

Offer patient online access as a possible solution for access

See Online Access Form

- Process copying – redact third party entries and entries considered harmful
- Practice to verify copying to confirm release

Copies of records released

All electronic request should be return electronically - send securely Via Email

If patient Collects Records complete form

If deemed excess or repetitive, or unable to clarify request send Letter to requestor explaining decision to decline

Process as Step-by-Step for Staff

- Check the Identity of the requestor, check if the Solicitor or insurance request has patient consent attached, if not reject, or seek patient consent from 3rd party, you can send Patient Access to Records form to clarify.

- Check if the request is under GDPR or Access to Medical Records Act (AMRA, this covers all employment, life insurance, mortgage insurance, insured negligence - anything covered by an insurance contract that requires a medical report). If it's an AMRA request, the standard (previous) fees still apply.

- Talk to the patient to negotiate the requested data - In most circumstances the patient is unlikely to want copies of the irrelevant historical paper records for themselves or to be sent to a 3rd party representing them. The patient may only want information from a certain date or for a date range or about a particular accident/incident, clarifying directly with the patient what is required may assist to reduce the amount of time taken to respond to a request.

- If the patient insists they need historical information that is not contained online (paper records, very old documents) check they are really required. We can negotiate with the patient about what information is provided but cannot refuse. We must print these out for the patient Free of Charge and are responsible for postage costs to a proxy if the volume of copies isn't 'excessive'. This isn't defined and would have to be justified but if is excessively weightier than average postage and admin costs can be changed.

- If it is a GDPR request, check if it's the first time the SAME information has been sent to ANY proxy (3rd party) of the patient, this includes solicitors. If identical info has been already sent, then this is a repeated request and can charge for a reasonable administration fee for a duplicate report.

- Speak with the patient and grant them Web online access to documents and consultations. This will provide them with the facility to view/print their information and will fulfil our obligations under the act.

- Provide them with a link to our Privacy Notice. This is on our website, if sending hard copies include a link in the covering letter and a copy of the PCIG "How we Use your information leaflet"

- If the patient has no internet access at all, print off the info requested and process/post at our expense, unless excessive or repeat request when a charge would be applicable.

- You could ask the patient to collect records and sign for them, providing ID and signing a collection form below.

- All posted copy records must also include our privacy notice.

Checking ID – Pausing the one-month Clock

Before access is provided the identity of the person making the request must be verified using 'reasonable means', you can use a form or check photo ID for this purpose.

Once the request has been received and verified, the individual must be provided with a copy of their data without undue delay, and at the latest within one month from the date of the request received.

Sometimes, additional information such as confirming the Identity of the requestor or the scope of the request is needed before copies can be supplied. In such cases, the one-month time limit will begin as soon as the additional information has been received

AMRA or GDPR request

Access to Medical Reports Act 1988 is an Act to establish a right of access by individuals to reports relating to themselves provided by medical practitioners for employment or insurance purposes and to make provision for related matters.

Check if the request is under GDPR or Access to Medical Records Act (AMRA, this covers all employment, life insurance, mortgage insurance, insured negligence - anything covered by an insurance contract that requires a medical report). If it's an AMRA request, the standard (previous) fees still apply.

There is a potential for requests that the practice feel are AMRA requests to be quoted as GDPR by 3rd parties, so PCIG would suggest seeking clarification from the Solicitors or companies involved if these are GDPR requests, however we feel in the main they will all probably state they are GDPR requests to avoid associated AMRA costs.

The problem is this, if a practice insists a request is under the AMRA requirements it runs the risk of a complaint to the ICO, or you wait for a response and if they say GDPR you absorb the costs.

Good Practice would be to email the solicitors asking for clarification of legal powers used to access the patient date using text such as the below: -

"The practice would like to clarify the purpose of this request. There are two forms of legislation relating to release of medical records, Access to Medical Reports Act which is usually for an insurance related reason or for employment purposes, this purpose still has a fee attached to process this request.

The other legislation is a subject access request under the GDPR legislation which as you rightly say is now not chargeable.

Therefore, could you please clarify your purpose for requesting these records, is this an Access to Medical Reports Act request which carries a fee or are you requesting these records as a Subject Access Request as part of the new GDPR legislation which doesn't incur a charge."

If you could please clarify the purpose and we will of course deal with your request without delay.

A patient can authorise a solicitor acting on their behalf to make a SAR. Health professionals releasing information to solicitors acting for their patients should ensure that they have the patient's written consent. Solicitors provide the patient's written consent. The consent must cover the nature and extent of the information to be disclosed under the SAR (for example, past medical history), and who might have access to it as part of the legal proceedings. Where there is any doubt, health professionals should confirm with the patient before disclosing the information. Should the patient refuse, the solicitor may apply for a court order requiring disclosure of the information.

Or you could seek clarification using the letter template below:-

Letter seeking Clarification

Dear <Company>,

Thank you for your Access Request on behalf of <Patient Name>. I note the signed consent of the patient for you to make this request.

I am writing to clarify the purpose of this request and whether the information you are requesting should be more properly requested under the Access to Medical Reports Act (AMRA) 1988, for which a recommended process is available as agreed with the Association of British Insurers (ABI) as below:

https://www.abi.org.uk/globalassets/sitecore/files/documents/publications/public/2017/health/requesting-and-obtaining-medical-information-electronically.pdf
specifically:

"In July 2015, the use of SARs for insurance purposes was reviewed by the Information Commissioner's Office (ICO) who expressed concerns regarding this process and possible Data Protection issues that it could potentially create".

Also, clauses 184 and 185 of the Data Protection Act 2018 has extended the offence of "enforced subject access" to cover medical records.

I would be grateful if you could confirm whether your request is for a SAR under Article 15 of the General Data Protection Regulation 2016, or is in fact better suited to an AMRA 1998 request as above?

Please note that, as a GDPR compliant Data Controller, the practice should only process requests for the release of personal data that are proportionate and relevant, and not excessive, for free within one month of receipt. We may refer this request to the patient for clarification of the data requested to be released to you in accordance with GDPR Recital 63 (*Where the controller processes a large quantity of information concerning the data subject, the controller should be able to request that, before the information is delivered, the data subject specify the information or processing activities to which the request relate*) or the ICO if appropriate.

Yours sincerely,

Requests from insurers

The BMA guidance May 2018 states: -

SARs from insurance companies to GP practices for the disclosure of full medical records is the subject of separate advice available on the BMA website. The position of the ICO is that the use of SARs to obtain medical information for life assurance purposes is an abuse of subject access rights and the processing of full medical records by insurance companies risks breaching the GDPR.

This does not mean, however, that GP data controllers can refuse to respond to a SAR from an insurer outright. When a SAR from an insurance company is received, the GP should contact the patient to explain the extent of the disclosure that has been sought. GPs can then, if requested, provide the patient themselves with their medical record rather than providing them directly to the insurance company. It is then the patient's choice as to whether, having reviewed the record, they choose to share it with the insurance company.

There is a clear distinction between the use of SARs by a solicitor, who can be seen as an agent of the patient and who is acting on the patient's behalf, and the use of SARs by insurance companies.

Insurance companies should use the provisions of the Access to Medical Reports Act 1988 to seek a GP report see full guidance on BMA website.

Excessive Requests

This isn't defined and would have to be justified but if is excessively wider request (as below) admin costs can be changed.

If you believe a request is 'manifestly unfounded or excessive' you can charge a fee or refuse to respond but will need to be able to provide evidence of how the conclusion that the request is excessive was reached. In most cases, you will not be able to charge for processing an access request, unless you can demonstrate that the cost will be excessive to the practice.

The latest guidance from the ICO suggests that the volume of information in a record would not be assessed in regards to an excessive claim (i.e. number of papers), but excessive is really based on the request – "please give me everything the practice holds on me" might be excessive as it includes CCTV, telephone recording, emails, letters and medical record. Whereas "please provide my medical record" would probably not be excessive.

Repeated requests

Initial access must be provided free of charge.

If SAME information has been sent to ANY proxy of the patient, this includes solicitors, the practice can charge for a reasonable administration fee for a duplicate report.

For supplying a copy, a fee not exceeding the cost of making the copy and postal costs may be charged. Charges should be reasonable and justifiable.

Health professionals may charge a professional fee to cover the costs of giving access to the records of deceased patients that is not covered by legislation. The GDPR does not apply to data concerning deceased persons.

Fees in General

According to the BMA :-

The circumstances when a fee can be charged for access to health records are likely to be rare and further advice should be sought on specific cases where it is believed that charging might be justifiable.

Supplying records directly to patients

Some practices have questioned if it is appropriate to supply records directly to the patient, and advise has been sought from the ICO on this matter, please see the advise received from the OIC below: -

10 August 2018

Case Reference Number

Dear

Thank you for your email of 16 July (attached for your reference).

In relation to Subject Access Requests (SAR) received from solicitors, the requests should only be being made by solicitors when they are acting on behalf of, and with the authority of, their clients. We would always recommend GP surgeries contact the patient to verify that the request is made with their consent. If the request has not been made on behalf of the individual, it will not be a valid request.

You should also inform the patient of the scope of the information requested and make sure the patient is aware of what the solicitors will receive if this is disclosed. If the patient wishes to proceed in making the SAR, the GP should comply with that request by supplying the records in question directly to their patient.

Clearly, if the patient chooses not to forward any particular part of their medical records to the solicitors then he or she does not want them to have that information. Consequently the supply of such information will not be done with the authority of the patient. If the solicitor is attempting to circumvent or manipulate this process to obtain medical records that they do not believe the patient wishes them to have, it is not a lawful SAR but potentially an unlawful attempt to obtain Special Category personal data.

I recommend that you continue with your current policy as the objection that you say has been raised by the solicitors is that they cannot get medical records the patient doesn't want them to have. A SAR is not designed to allow third parties to obtain personal data the data subject does

not want disclosed so you should continue to resist attempts to obtain personal data without consent in this manner.

If the solicitor is concerned that their client is not providing them with all the medical information they require that is a matter for them to resolve directly with their client.

I hope this information is helpful to you. If you would like to discuss this enquiry further, please contact me on my direct number 0330 414 6484. If you need advice on a new issue you can contact us via our Helpline on 0303 123 1113 or through our live chat service. In addition, more information about the Information Commissioner's Office and the legislation we oversee is available on our website at www.ico.org.uk. For information about what we do with personal data see our privacy notice.

Yours sincerely

Caitlin Muir
Lead Case Officer
Information Commissioner's Office

Using this response, the practice has created a simple response to solicitors who request records directly and have been unhappy when copies have been sent to or clarification sought from the patient.

Dear Xxxxx

Thank you for your honesty about the reason for requesting a SAR on behalf of the patient.

Our process is in line with the advice we have received from the ICO. This advice is being used to inform and update the BMA guidelines accordingly.

I have pasted the advice directly below for your reference.

If this is a SAR for the purpose of the GDPR then we will happily provide the patient with electronic access to their record. If the patient is unable to access the electronic portal, then we can provide a printed copy that we can provide directly to the patient.

As I have flagged below this is often unacceptable to solicitors for the purposes of compiling a medical report from the record in case the record is tampered with.

If you would like a copy of the record provided directly to you, we can do this with the patient explicit consent, but this is not cover

by the SAR and is therefore chargeable

I look forward to hearing how you would like to move forward.

Many Thanks

Redaction or editing out Information

The GDPR read together with the forthcoming Data Protection Act 2018 provides for several exemptions in respect of information falling within the scope of a SAR. In summary, information can generally be treated as exempt from disclosure and should not be disclosed, if:

- it is likely to cause serious physical or mental harm to the patient or another person; or – it relates to a third party who has not given consent for disclosure (where that third party is not a health professional who has cared for the patient) and after taking into account the balance between the duty of confidentiality to the third party and the right of access of the applicant, the data controller concludes it is reasonable to withhold third party information; or

- it is requested by a third party and, the patient had asked that the information be kept confidential, or the records are subject to legal professional privilege or, in Scotland, the records are subject to confidentiality as between client and professional legal advisor. This may arise in the case of an independent medical report written for the purpose of litigation. In such cases, the information will be exempt if after considering the third party's right to access and the patient's right to confidentiality, the data controller reasonably concludes that confidentiality should prevail; or

- it is restricted by order of the courts; or

- it relates to the keeping or using of gametes or embryos or pertains to an individual being born as a result of in vitro fertilisation; or

- in the case of children's records, disclosure is prohibited by law, e.g. adoption records.

The data controller must redact or block out any exempt information

TEMPLATE PATIENT RESPONSE SAR LETTER

Dear Sir/Madam,

Access to Health Records under the General Data Protection Regulations 2016

Below is background information regarding your rights under the Data Protection Act 2018 in relation to requesting access to your health records, along with a form to assist you to make your request.

The General Data Protection Regulation 2016 (GDPR) and Data Protection Act 2018 gives every living person, or an authorised representative, the right to apply for access to health records. A request should be made (this includes e-mail) to the data controller at the NHS organisation where your records are held. Please contact us for alternative methods of obtaining access if you are unable to make a request in writing.

Under the GDPR, there is NO fee to view your health records or to be provided with a copy of them.

We are not obliged to comply with your access request unless:

- we have sufficient information to identify you and to locate the information held about you.
- if your request is deemed to be repetitive (i.e. you have already received your information in the Past 12 months)
- it is excessive in nature for excessive requests based on a case-by-case judgement we may pass on our administrative costs.
-

Once we have all the required information, where relevant, your request will be dealt with within one month. In exceptional circumstances, where it is not possible to comply with this timeframe, you will be informed of the delay and given a timescale of no longer than a further two months from the date of request for when your request is likely to be met. If you choose to share your information with anyone else, this will be at your own risk

In some circumstances, the legislation permits us to withhold information held in your health records. These rare cases are:

- Where it has been judged that supplying you with the information is likely to cause serious harm to the physical or mental health or condition you, or any other person, or;
- Where providing you with access would disclose information relating to or provided by a third person who had not consented to the disclosure, this exemption does not apply where that third person is a health professional involved in your care.

When making your request for access, it would be helpful if you could provide details of the periods and parts of your health record you require. Although this is optional, it will help save NHS time and resources, and may avoid the issue of excessive requests and associated costs.

If you are using an authorised representative, you need to be aware that in doing so they may gain access to all health records concerning you, which may not be relevant. If this is a concern, you should inform your representative of what information you wish them to specifically request when they are applying for access.

If you have any complaints about any aspect of your application to obtain access to your health records, you should first discuss this with the practice. If this proves unsuccessful, you can make a complaint through the NHS Complaints Procedure by contacting the NHS organisation formally.

Further information about the NHS Complaints Procedure is available on the NHS Choices website at: www.nhs.uk/aboutNHSChoices/pages/Howtocomplaincompliment.aspx

Alternatively, you can contact the Information Commissioners Office (responsible for governing Data Protection compliance) at: Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF, Tel 01625 545700, or www.ico.org.uk .

Yours sincerely

Ops Manager

Access to Medical Record Request Form

Date Received		
Date Due to be completed by (One Month)		
Patient: Name DOB Address NHS Number		
Name of Requestor	How is the request made? If request received electronically, information should be provided in a commonly used electronic format.	Request received: Writing Email Verbally Other.
Access Details	Access under General Data Protection Regulations 2016/679 (free) Access to Medical Reports Action (AMRA) 1990 (Chargeable) i.e. reports for employment and insurance purposes includes cover for accident claims, insured negligence, mortgage and life insurance. Anything covered by an insurance contract to support actual or potential insured claim then AMRA applies. If requestor letter does not specify precise purpose of request contact requestor to clarify: "The practice has received your request for named patient, I require further clarification: • The Purpose this is being requested for • Which legislation is the request being made under: DGPR (free) or AMRA (chargeable) "	Yes/No Yes/No
Details of Request	Entire Medical Records Dates: From To	
Verification of Authority/Patient consent	Requester's Identity confirmed: Yes/No Requester's legal authority confirmed: Yes/No	

	Patient's identity verified: Yes/No If Patient does not have capacity – verify: Enduring Power of Attorney: Yes/No Lasting Power of Attorney for Health and Welfare: Yes/No Court Appointed Deputy: Yes/No	
Contact with Patient	Date of Patient Contact: "It is my duty to discuss the recent request made by …… with you and to advice you what information will be provided, that we hold for you on your computer records and in your paper records – it is your choice to decide the amount of information we provide to the requestor – this can be your entire medical records, from a specific date. Discussed type of information held by the practice which can include – • Demographic data: Yes /No • Diagnoses/investigation results: Yes/No • Procedural and consultation information recorded by practice and ancillary colleagues e.g. D/Nurse Health Visitor: Yes/No • Immunisations and medications: Yes/No • All letters: Yes/No • Sensitive information – Sexual health and mental health access: Yes/No • All third party information will be removed i.e. Any references to named individuals – spouses, children etc. Patient confirms requestors request If No – details of patient's new request: Proposed date given when medical copies will be released:	Yes /No
Confidential Third-party information removed/redacted	Yes – Details of information removed No	
If Subject Access Request refused – contact Practice Data Protection Officer Paul Couldrey, PCIG Consulting Ltd Tel: 07525623939.	Date of contact with Data Protection Officer: Date of refusal letter:	
GP confirmation for release of Medical Records	Name of GP: Request authorised: Patient Details validated: Copies of Medical Records validated for third party	 Yes/No Yes/No

	information/sensitive information and redaction complete: Request authorised for release: GP Signature…… Date:	Yes/No Yes/No
Date of completed request		

Access to GP Online Services Form

Surname			
First name			
Date of birth			
Address			
Postcode			
Email address			
Telephone number		Mobile number	

I wish to have access to the following online services (tick all that apply):

Booking appointments	☐
Requesting repeat prescriptions	☐
Accessing Test Results, Immunisations and Problems	☐

Application for online access to my medical record

I wish to access my medical record online and understand and agree with each statement (please tick)

I have read and understood the information on the reverse of this form	☐
I will be responsible for the security of the information that I see or download	☐
If I choose to share my information with anyone else, this is at my own risk	☐
I will contact the practice as soon as possible if I suspect that my account has been accessed by someone without my agreement	☐
If I see information in my record that is not about me, or is inaccurate I will log out immediately and contact the practice as soon as possible	☐

Signature		Date	

For practice use only

Identity verified through (tick all that apply)	Vouching ☐ Vouching with information in record ☐ Photo ID ☐ Proof of residence ☐	Name of Verifier	Date
Staff Name authorising Access			Date

Important Information – Please read before returning this form

If you wish, you can now use the internet/mobile phone to book appointments with a GP, request repeat prescriptions for any medications you take regularly and look at your medical records all online. Also, you can still use our website or call the surgery for any queries regarding the above services. It's your choice.

It will be your responsibility to keep your login details and password safe and secure. If you know or suspect that your record has been accessed by someone that you have not agreed should see it, then you should change your password immediately.

If for any reason you cannot do this, we recommend that you contact the practice so that they can remove your online access until you are able to reset your password.

If you print out any information from your records, it will be your responsibility to keep this safe and secure. If you are at all worried about keeping printed copies safe and secure, we recommend that you do not make copies at all.

Before you apply for online access to your record, there are some other things to consider.

Although the chances of any of the following happening are very small, you will be asked if you have read and understood the following before you are given login details from our Staff Member.

Forgotten history There may be something you have forgotten about in your record that you might find upsetting.
Abnormal results or bad news If your GP has given you access to test results or letters, you may see something that you find upsetting to you. This may occur before you have spoken to your doctor or while the surgery is closed and you cannot contact them.
Choosing to share your information with someone It's up to you whether or not you share your information with others – perhaps family members or carers. It's your choice, but also your responsibility to keep the information safe and secure.
Coercion If you think you may be pressured into revealing details from your patient record to someone else

against your will, it is best that you do not register for access at this time.

Misunderstanding Medical Information

Your medical record is designed to be used by clinical professionals to ensure that you receive the best possible care. Some of the information within your medical record may be highly technical, written by specialists and not easily understood. If you require further clarification, please contact the surgery for a clearer explanation.

Information about someone else

If you spot something in the record that is not about you or notice any other errors, please log out of the system immediately and contact the practice as soon as possible.

Further Information

For more information about keeping your healthcare records safe and secure please visit our website: **[SURGERY WEB ADDRESS]**

Patient Collecting Requested Medical Records Form

PATIENT DISCLAIMER: I confirm that I have received the requested copies of my Medical Records. I accept full responsibility for the safety and security of these records.

Name of Staff Member Handing over the Records	
Signature of Staff Member	
Date	
Time	
Name of Applicant	
Signature of Applicant	

(For office use only)

When the above has been completed please scan in patients records – OR – records in coded entry of Medical Record that SAR has been collected.

NHS.net How to send an encrypted message to non-NHS.net Account

Before sending patient or sensitive data via the encryption service, it is good practice to set up the 'encrypted channel' which helps safely verify the correct recipient.

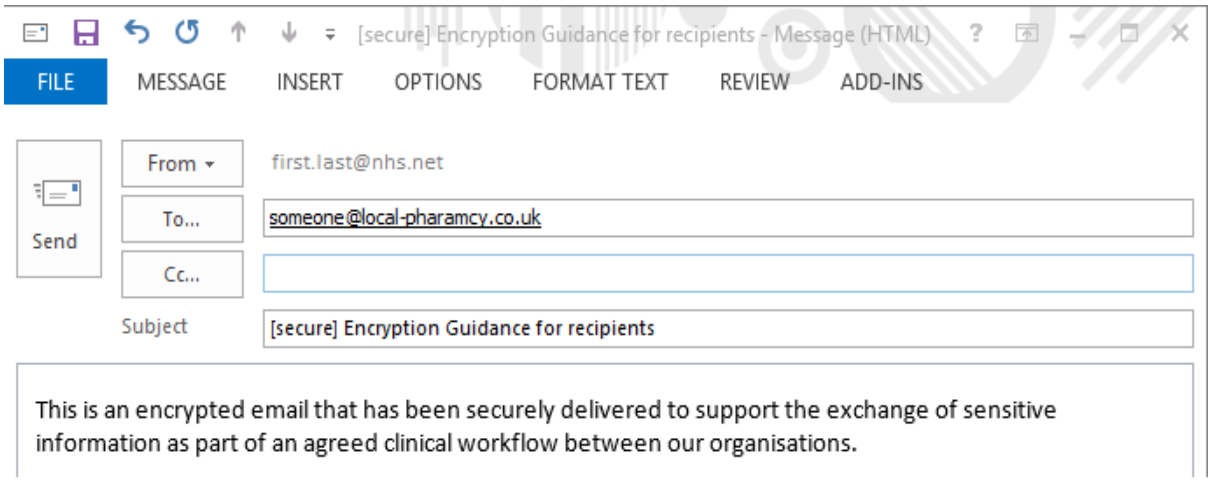
1. First, send the recipient the 'Encryption Guidance for recipients' document which you can find in the NHSmail Training and Guidance pages at: https://web.nhs.net/Portal/InformationGuidanceServices/DefaultPage.aspx in the section 'Emailing sensitive or patient identifiable information'.

2. Next, follow the steps below to send an initial encrypted email but do not include patient or sensitive information. Once the recipient of the information has registered for the encryption service and confirmed to the sender this has been done, patient and sensitive data can be sent within an email or as an attachment subject to local information governance policies.

3. To send an encrypted email, log into your NHSmail account (either via an email client such as Outlook or via the web portal at www.nhs.net) and create a new email message in the normal way.

4. Ensure the recipient's email address is correct

5. In the Subject field of the email, enter the word [secure] before the subject of the message. The word secure must be surrounded by the square brackets for the message to be encrypted. If square brackets aren't used, the content of the email will be sent in plain text and may potentially be exposed to interception or amendment.



6. Compose the message

7. Add any required attachments (once the initial registration process has taken place)

8. Click on Send to send the message. An unencrypted copy will be saved in your Sent Items folder.

The service will then encrypt the message and deliver it to the intended recipient. The sent item will be stored unencrypted in your Sent Items folder, and any replies received will be decrypted and displayed as normal in NHSmail.

N.B. [secure] is not case sensitive and [SECURE] or [Secure] for example could also be used.